

ПОЛОЖЕНИЕ

об организации системы охранного телевидения (видеонаблюдения) на объектах (территориях) ГБУЗ РК «Евпаторийская городская больница»

1. Общие положения

1.1. Настоящее Положение определяет задачи, цели, способы и порядок осуществления видеонаблюдения, порядок доступа к видеоматериалам, порядок хранения и уничтожения видеоматериалов и разработано в соответствии с:

Конституцией Российской Федерации;

Федеральным законом № 323-ФЗ от 21.11.2011 г. основах охраны здоровья граждан в Российской Федерации;

Законом РФ от 11.03.1992г. № 2487-1 «О частной детективной и охранной деятельности в Российской Федерации»;

- Федеральным Законом от 27.07.2006г. 152-ФЗ «О персональных данных»;

- Постановлением Правительства РФ от 17.11.2007 г. № 781 утверждения Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных;

- Постановлением Правительства РФ от 13.01.2017г. № 8 «Об утверждении требований к антитеррористической защищенности объектов (территорий) Министерства здравоохранения Российской Федерации и объектов (территорий), относящихся сфере деятельности Министерства здравоохранения Российской Федерации, и формы паспорта безопасности этих объектов (территорий)»;

1.2. Под видеонаблюдением понимается непосредственное осуществление видеонаблюдения с использованием видеокамер для получения видеoinформации об объектах и помещениях, а также запись полученного изображения и его хранение для последующего использования.

1.3. Организация видеонаблюдения на территории ГБУЗ РК «Евпаторийская городская больница» (далее по тексту - Учреждение) является элементом общей системы безопасности Учреждения, направленной на обеспечение безопасности осуществления медицинской деятельности, сохранение жизни и здоровья пациентов и сотрудников, поддержание трудовой дисциплины и порядка, предупреждение возникновения несчастных случаев, пожаров, аварий и других чрезвычайных ситуаций.

Система видеонаблюдения является открытой и не может быть направлена на сбор информации о конкретном человеке.

Учреждение обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных», и принятыми в соответствии с ним нормативными правовыми актами.

Видеонаблюдение должно проводиться без идентификации снятых на видеозапись изображений людей. До передачи материалов видеосъемки для установления личности снятого человека органами, ведущими оперативно-розыскную деятельность, дознание и следствие, видеонаблюдение не считается обработкой биометрических персональных данных и на её проведение письменного согласия не требуется.

1.7. Настоящее Положение обязательно для сотрудников, пациентов, посетителей Учреждения, а также сотрудников организации, осуществляющей техническое обслуживание приборов систем видеонаблюдения.

2. Порядок организации системы видеонаблюдения

2.1. Решение об установке СОТ (системы охранного телевидения) принимается главным врачом Учреждения.

2.2. Запрещается использование устройств, предназначенных для негласного получения информации (скрытых камер).

2.3. О ведении видеонаблюдения сотрудники, пациенты и посетители Учреждения оповещаются соответствующими надписями и (или) символами, размещаемыми в доступных местах.

2.4. Записи видеонаблюдения ведутся в автономном режиме, хранятся и автоматически уничтожаются в соответствии с техническими характеристиками установленного оборудования и программного обеспечения в установленный законом срок.

2.5. Приказом главного врача Учреждения из числа работников назначается ответственный за внедрение системы видеонаблюдения и её функционирование.

3. Задачи и цели системы видеонаблюдения

3.1. Система видеонаблюдения призвана выполнять следующие задачи:

- повышение эффективности действий при возникновении нештатных и чрезвычайных ситуаций; обеспечение мер по усилению антитеррористической и противопожарной защиты;
- обеспечение защиты сотрудников, пациентов, посетителей и территории Учреждения, охраны порядка и безопасности;
- исключение бесконтрольного пребывания в Учреждении посторонних лиц и нахождения на его территории транспортных средств, в том числе в непосредственной близости от объекта (территории);
- пресечение противоправных действий, которые могут нанести вред имуществу Учреждения, а также посетителям, сотрудникам и пациентам;
- своевременное выявление фактов нарушения пропускного и внутриобъектового режимов, попыток проноса и провоза запрещенных предметов (радиоактивных, взрывчатых, отравляющих веществ, оружия, боеприпасов, наркотических средств и других опасных предметов и веществ) на объект (территорию), предотвращение попыток их оборота, распития спиртных напитков, курения.

3.2. Видеонаблюдение осуществляется с целью:

- документальной фиксации возможных противоправных действий;
- обеспечения антитеррористической безопасности;
- осуществления внутреннего контроля качества, доступности предоставляемых услуг и безопасности медицинской деятельности.

3.3. Материалы видеозаписей, полученных камерами видеонаблюдения, в случае необходимости могут использоваться в качестве доказательства в уголовном, административном или гражданском судопроизводстве для доказывания факта совершения противоправного действия, а также для установления личности лица, совершившего соответствующее противоправное действие.

4. Порядок информирования о функционировании и использовании системы видеонаблюдения

4.1. Лица, являющиеся сотрудниками на момент утверждения настоящего Положения, знакомятся с настоящим Положением под роспись в структурных подразделениях организации.

4.2. Сотрудники, вновь принимаемые на работу, знакомятся с настоящим Положением под роспись в отделе кадров.

4.3. Посетители и пациенты информируются о работе системе видеонаблюдения путем размещения специальных информационных табличек на входе в Учреждение и на объектах Учреждения.

4.4. Положение размещается на официальном сайте Учреждения, выдержки из Положения на информационных стендах структурных подразделений Учреждения.

5. Состав системы видеонаблюдения

5.1. Система видеонаблюдения состоит из:

- видеокамер открытого наблюдения, установленных внутри здания;

- видеорекамер открытого наблюдения, установленных на здании; - видеорекамер открытого наблюдения, установленных на территории;
- серверов хранения видеоматериалов;
- программного комплекса записи, хранения и доступа к видеоматериалам; - сети передачи данных;
- источников бесперебойного питания.

5.2. Видеоматериалы записываются с помощью программно-аппаратного комплекса, установленного в помещении ограниченного доступа (серверная) в здании Учреждения. Доступ к видеоматериалам по сети общего доступа (Интернет) не допускается.

6. Порядок ведения видеонаблюдения

6.1. Видеонаблюдение ведется открытым способом. Скрытое видеонаблюдение запрещается.

6.2. Программно-аппаратный комплекс видеонаблюдения функционирует круглосуточно в автоматическом режиме и обеспечивает сохранность и неизменность данных видеонаблюдения.

6.3. Расположение камер и постоянный режим записи (постоянный или по движению) определяется необходимостью ведения видеонаблюдения за контролируемыми зонами, по согласованию с заместителем главного врача по безопасности.

6.4. Видеоизображения со всех камер синхронизируются по времени видеосервера.

7. Порядок доступа к записям системы видеонаблюдения

7.1. Передача записей камер видеонаблюдения третьей стороне допускается только в исключительных случаях, включая запросы правоохранительных и (или) судебных органов. Вопрос о передаче записей решает главный врач Учреждения, руководствуясь действующим законодательством Российской Федерации.

7.2. К просмотру видеoinформации допускаются:

- работники сторонней организации, состоящей с медорганизацией в договорных отношениях с целью выполнения возложенных на них обязанностей по техническому сопровождению;

- работники охраны Учреждения, имеющие право просмотра видеoinформации только в режиме онлайн в рамках своих должностных обязанностей, в период своего рабочего времени (дежурства);

- главный врач, заместитель главного врача, специалист по защите информации, сотрудники отдела информационных технологий, с целью выполнения возложенных на них должностных обязанностей;

- представители уполномоченных органов, с целью использования изображений для осуществления государственных, общественных или иных публичных интересов. Представители уполномоченных органов допускаются до просмотра видеозаписей на основании письменного запроса, оформленного в соответствии с требованиями законодательства в сфере защиты персональных данных, с разрешающей резолюцией главного врача больницы либо лица исполняющего его обязанности, в присутствии уполномоченного должностного лица медорганизации. Передача копии видеозаписи может осуществляться только уполномоченным органам (контрольно-надзорные органы, судебные органы) в порядке, установленном к передаче сведений, содержащих персональные данные;

7.3. Срок хранения видеозаписей составляет 30 дней (постановление Правительства от 25.03.2015г. № 272), после этого срока запись подлежит уничтожению. Если камеры видеонаблюдения зафиксировали конфликтную (нестандартную) ситуацию, то для таких записей устанавливается специальный срок хранения по распоряжению руководителя или разъяснения ситуации. Если камеры зафиксировали конфликтную ситуацию между посетителем и сотрудником ГБУЗ РК «Евпаторийская городская больница» то такие записи подлежат хранению в течение срока исковой давности, т. е. в течение трех лет.

8. Порядок обработки персональных данных, полученных в результате видеонаблюдения

8.1. Доступ к записям видеонаблюдения при возникновении конфликтных ситуаций осуществляется ответственным за её функционирование сотрудником или главным врачом Учреждения. Сотрудники Учреждения не вправе предоставлять доступ к мониторам видеокамер (видеоинформации), иным способом сообщать сведения и конфиденциальную персональную информацию, ставшую им известной при работе с системой видеонаблюдения, третьим лицам, не уполномоченным в установленном порядке на ее получение.

8.2. При заключении договорных отношений со сторонней организацией на техническое сопровождение системы видеонаблюдения, договор должен содержать условие о неразглашении работниками сторонней организации информации, полученной при просмотре видеозаписей, включая персональные данные и/или врачебную тайну.

9. Меры по обеспечению безопасности персональных данных

9.1. В тех случаях, когда система видеонаблюдения позволяет отслеживать деятельность работников на рабочем месте или в иных помещениях, закрытых для общего доступа, такое наблюдение будет считаться обработкой персональных данных.

9.2. Учреждение обязуется принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами.

9.3. Обработка персональных данных должна осуществляться на законной основе и ограничиваться достижением конкретных, заранее определенных и законных целей. Не допускается обработка персональных данных, не совместимая с целями сбора персональных данных.

9.4. Хранение персональных данных должно осуществляться не дольше, чем этого требуют цели обработки персональных данных. Обрабатываемые персональные данные подлежат уничтожению либо обезличиванию по достижении целей обработки или в случае утраты необходимости в достижении этих целей.

10. Ответственность за нарушение правил обработки персональных данных

10.1. Лица, виновные в нарушении требований настоящего Положения, несут предусмотренную законодательством Российской Федерации ответственность.

10.2. Лицо, виновное в причинении вреда нарушением конфиденциальности записей камер, несет ответственность в порядке, предусмотренном действующим законодательством Российской Федерации.

10.3. Вопросы, не урегулированные условиями настоящего Положения, регулируются на основе Федерального закона Российской Федерации от 27 июля 2006 года 152-ФЗ «О персональных данных» и иных нормативных правовых актов регулирующих данную сферу правоотношений.